Tasmanian Government

Identity and Access Management Toolkit

Part 3

Identity Credential Management Guidelines and Standards

Department of Premier and Cabinet

Tasmania
Explore the possibilities

For further information on the Toolkit, contact the Office of eGovernment:

egovernment@dpac.tas.gov.au | www.egovernment.tas.gov.au

ISBN:
978 0 7246 5580 8: Tasmanian Government Identity and Access Management Toolkit – PDF
978 0 7246 5586 7: Tasmanian Government Identity and Access Management Toolkit – HTML

Contents

Using the Identity Credential Management Guidelines and Standards

Part 3 – Credential Management Guidelines and Standards forms part of the *Identity and Access Management Toolkit* and provides guidelines to assist agencies in selecting the best form of credential that is fit for purpose and matches the level of risk associated with the service and the intended use of that credential.

A credential might take different forms, depending on the nature of the service and the need for registered users of that service to provide evidence of that registration. Examples of credentials issued by the Tasmanian Government include plastic cards (eg driver's licence, Seniors Card), a paper document (eg registration certificate, birth certificate), vehicle stickers (eg an endorsed registration sticker showing a receipt number), or a certificate of competency (eg education certificate, business affairs certificate).

Similarly to identity enrolment or registration, the processes to be applied to the issuing and management of credentials is risk-based.

As with Part 2 of the Toolkit, Part 3 provides guidelines for each credential assurance level, together with standards in relation to both electronic and non-electronic identity credentials.

Section 1

Identity Credential Management Guidelines

Credential Assurance Level 4 Guidelines

Suitable for:

The following processes are relevant for any of the credentials or documents issued under the Identity Registration Assurance Level 4 in Part 2 of the Identity and Access Management Toolkit.

It should be noted that some of the following procedures for a Credential Assurance Level 4 do not apply to a Birth Certificate.

1. Generating the credential and updating the directory

- An issuing order to generate a credential will be made only on receipt of a written request from the identity enrolment agency
- The issuing order will contain relevant information as required by the agency, and consistent with Credential Assurance Level 4 (CAL-4) standards or requirements, including:
  - Unique identifying number for the client or service
  - The client's name in the format to be included on the credential (and consistent with agreed whole-of-government requirements – eg AS4590)
  - Other relevant client data, such as date of birth, address, etc, required by the agency
  - Biometric feature, such as photograph
- If not already created, a client record should be created in an agency client information store[1], based on the information provided in the issuing order (see *Information Security Guidelines*, Version 4.0, February 2008)
- If the credential is to be produced by an external supplier, the order should be submitted in a secure manner, as provided under *Information Security Guidelines* (version 4.0, February 2008, section 6.3.1) and in accordance with the requirements of the *Personal Information Protection Act 2004* (available at www.thelaw.tas.gov.au)
- Once produced, the credential should be returned to the credential issuing agency for checking prior to distribution to the client, particularly to verify the accuracy of information printed on the credential against the initial instructing order, and the fitness for purpose of the relevant security features
- When the credential is ready to send to the client, the client's record in the agency directory needs to be updated to establish the link between the client and the credential
- Prior to delivery of the credential to the client, it should be stored securely in accordance with the *Information Security Guidelines*, Section 3, Record Security Guidelines, and Section 4, Physical Security Guidelines)
- The credential to be issued should incorporate a two factor authentication process, one of which should be a biometric factor, for example a photograph, fingerprint, iris scan, etc (see the *Identity Credential Standards* at section 2 of this part of the Toolkit)

[1] Referred to in future as the directory

2. Delivery and activation of the credential

- The credential would be delivered to the client by either:
  - Post or by courier - the client, or their nominated agent, should be required to sign for or otherwise acknowledge receipt
  - Collected in person by the client – the client, or their nominated agent, should be required to provide evidence of their authority to collect the credential. This evidence could be in a form designated at the time of registration, such as a signature plus photographic identification, each of which can be verified with the original application, as well as the credential being issued, if required
- A credential may be instantly issued while the client waits in emergency situations and where defined authentication and enrolment processes are applied to ensure that the identity being asserted at enrolment is correctly attributed to the person presenting to the agency
- The agency directory should be updated to show that the credential has been issued to the client, and the method of delivery
- At the time of issuing the credential, clients should be provided with details on what actions they are required to take to report lost, stolen or damaged credentials
- For security reasons, the client may be required to take specific action to activate the credential before it becomes accepted by the issuing agency
- Acceptable methods of activation are:
  - By telephone – based on specific prompts and the provision of authenticating information
  - By initial use – this might be based on the application of a password and/or PIN to the credential
  - Online – based on specific prompts and the provision of authenticating information
  - By SMS – based on the provision of particular information
- The appropriate method for activating a credential will be largely based on the type of credential involved and how it is intended to be used by the client in relation to the delivery of services
- Where a credential is required to be activated before it is current, the directory should be updated when the credential has been activated to show this fact

3. Recognising and verifying the credential

- Acceptable methods for identifying and/or verifying a CAL-4 credential include:
  - Online transaction – accompanied by a password, PIN, cryptographic keys and / or digital certificate
    Online transactions will require validation of the electronic credential using appropriate authentication protocols
  - Telephone transaction – by supplying the name on card, service and/or credential number, and keypad entry of PIN (if required)
    Telephone transactions will require a knowledge-based authentication process
    Knowledge-based authentication is not as secure as credential-based authentication and should be carefully considered in relation to the Level 4 assurance process
    Information to enable knowledge-based authentication needs to be collected during the enrolment process

  - In person transaction – accompanied by sighting the credential and the use of password or PIN (if required)
    In person transactions may use either credential-based or knowledge-based authentication. Credential-based authentication is recommended for Level 4 assurance processes

- Where a client's transaction with the system is over an extended period of time, for example longer than 30 minutes, or where the client moves to another secure area within the system, they should be required to re-authenticate
- It is recommended that clients are disconnected from a service after a pre-determined period of inactivity. This will reduce the risk of others using the client's credential
- When a client's session with a service has ended, there must be a process for recognising they have left or logged out in accordance with the Access Management Guidelines (see Part 4 of the Toolkit)
- The directory should be updated to show any credential activity, including client password and / or PIN changes
- A process for tracking any verification requests made (ie an audit trail) should be maintained
- CAL- 4 documents must be able to be verified with the issuing agency

4. Renewing / replacing the credential

- A CAL-4 credential would be issued with a set period of currency
- The client may be informed near to the period of expiration that the credential needs to be renewed
- Where a renewal notice or other form of notification is sent to the client, the directory should be updated accordingly to show that this was sent
- The notification would inform the client of relevant details, including:
  - The process required to renew the credential – eg payment of a fee, presentation of a photograph in a specified form, any authentication or POI requirement, return of the credential
  - Where to present in person, if required
  - What POI information to bring to the interview
- Once the required renewal procedures have been completed and the new credential has been renewed, the directory should be updated accordingly

5. Cancelling and/or replacement of lost, stolen or damaged credential

- A credential may be replaced within the set renewal period in situations where it is damaged or rendered unusable, but only on the basis of an established authentication process to verify the identity of the person requesting the replacement
- Clients would be required to report the loss or theft of a credential as soon as practicable after the event
- Replacing a lost or stolen credential poses a higher risk than replacing a damaged or unusable credential
- A credential may be replaced within the set renewal period in situations where it has been either lost or stolen, but only on the basis of an established authentication process that verifies the identity of the person requesting the replacement.
- On receiving notification of the loss or theft of a credential, the agency will:

  - Cancel the credential immediately
  - Update the directory to indicate the cancellation of credential, together with any other relevant details
- The client is informed of the steps they need to take to obtain a replacement credential (see sub-section 4 above)
- Where a client reports that the credential is extensively damaged rendering it unusable (eg water soaked), the agency will:
  - Require the client to present the damaged credential in person at a designated place
  - Retain the damaged credential
  - Provide the client with details of what requirements will apply – eg completion of statutory declaration, presentation of identification information, provision of photograph, etc
- When the requirements for reissuing the credential have been met, a credential can be reissued following the renewal/replacement procedure (see sub-section 4 above)
- When replacing a lost, stolen or damaged credential, it is desirable that a unique identification number or other feature be incorporated in the replacement credential to indicate its status as a replacement
- Where a damaged credential is returned and a replacement issued, the directory will be updated accordingly

6. Exceptions

As noted in Part 2 of the Toolkit, agencies will from time to time enrol clients who are not able to meet the required Identity Registration Assurance Level. In instances where a non-standard enrolment process is completed, it may also be necessary to issue a credential.

6.1 Non-standard applications

For medium to high risk situations, a credential issued under a non-standard identity assessment process should be issued only as a last resort and the risk associated with the transaction carefully considered by the agency or specific business unit responsible for the service or transaction.

One option is to issue the applicant with a restricted identity credential, which entitles the holder to access the issuing agency's services only, or which is issued only as a temporary credential with a limited period of currency.

6.2 Service - only credential

Where a registering agency has the need to implement a service-only or temporary credential, it would be appropriate to apply limitations on the credential, such as:

- It would lapse after a limited period of time, either when the individual was able to register to IRAL-4, or when the registration expires
- It would be issued for the sole purpose of doing business with the registering agency

In all instances of non-standard applications, the key consideration for the registering agency is that the applicant be required to provide evidence or documentation to the satisfaction of the registering agency and to a level determined by that agency but within the required constraints for an IRAL-4 registration.

Credential Assurance Level 3 Guidelines

Suitable for:

The following processes are relevant for any of the credentials or documents issued under the Identity Registration Assurance Level 3, as described in Part 2 of the Identity and Access Management Toolkit.

1. Generating the credential and updating the directory

- An issuing order to generate a credential will be made only on receipt of a written request from the identity enrolment agency
- The order should contain relevant information as required by the agency, and consistent with Credential Assurance Level 3 (CAL-3) standards or requirements, including:
  - Unique identifying number for the client or service
  - The client's name in the format to be included on the credential (and consistent with agreed whole-of-government requirements – eg AS4590)
  - Other relevant client data, such as date of birth, address, etc, required by the agency
  - Biometric feature, such as photograph
- If not already created, a client record should be created in an agency client information store (or directory), based on the information provided in the issuing order (see *Information Security Guidelines*, Version 4.0, February 2008)
- If the credential is to be produced by an external supplier, the order should be submitted in a secure manner, as provided under the *Information Security Guidelines* and in accordance with the requirements of the *Personal Information Protection Act 2004* (available at www.thelaw.tas.gov.au)
- Once produced, the credential should be returned to the credential issuing agency for checking prior to distribution to the client, particularly to verify the accuracy of information printed on the credential against the initial instructing order, and the fitness for purpose of the relevant security features
- When the credential is ready to send to the client, the client's record in the agency directory needs to be updated to establish the link between the client and the credential
- Prior to delivery of the credential to the client, it should be stored securely in accordance with the *Information Security Guidelines* (section 3, Record Security Guidelines, and section 4, Physical Security Guidelines)
- The credential to be issued should incorporate a two factor authentication process, one of which should be a biometric factor, for example a photograph, fingerprint, iris scan, etc (see the *Identity Credential Standards* at section 2 of this part of the Toolkit)

2. Delivery and activation of the credential

- The credential should be delivered to the client by either:
  - Post or by courier – it is recommended that the client, or their agent, be required to sign for or otherwise acknowledge receipt

  - Collected in person by the client – it is recommended the client, or their nominated agent, be required to provide evidence of their authority to collect the credential. This evidence could be in a form designated at the time of registration, such as a signature plus photographic identification, each of which can be verified with the original application, as well as the credential being issued, if required

- A credential may be instantly issued while the client waits, but only where it is accompanied by increased authentication and enrolment processes to ensure that the identity being asserted at enrolment is correctly attributed to the person presenting to the agency
- The agency directory should be updated to show that the credential has been issued to the client
- At the time of issuing the credential, clients should be provided with details of what actions they are required to take to report lost, stolen or damaged credentials
- For security reasons, the client may be required to take specific action to activate the credential before it becomes accepted by the issuing agency
- Acceptable methods of activation would be:
  - By telephone – based on specific prompts and the provision of authenticating information
  - By initial use – this might be based on the application of a password and / or PIN to the credential
  - Online – based on specific prompts and the provision of authenticating information
  - By SMS – based on the provision of particular information
- The appropriate method for activating a credential will be largely based on the type of credential involved and how it is intended to be used by the client in relation to the delivery of services
- Where a credential is required to be activated before it is current, the directory should be updated when the credential has been activated to show this fact

3. Recognising and verifying the credential

- Acceptable methods for identifying and/or verifying a CAL-3 credential include:
  - Online transaction – accompanied by a password, PIN, cryptographic keys and/or digital certificate
    Online transactions will require validation of the electronic credential using appropriate authentication protocols
  - Telephone transaction – by supplying the name on card, service and/or credential number, and keypad entry of PIN (if required)
    Telephone transactions will require a knowledge-based authentication process
    Knowledge-based authentication is not as secure as credential-based authentication and should be carefully considered in relation to the Level 4 assurance process
    Information to enable knowledge-.based authentication needs to be collected during the enrolment process
  - In person transaction – accompanied by sighting the credential and the use of password or PIN (if required)
    In person transactions may use either credential-based or knowledge-based authentication. Credential-based authentication is recommended for Level 4 assurance processes
- Where a client's transaction with the system is over an extended period of time, for example longer than 30 minutes, or where the client moves to another secure area within the system, they should be required to re-authenticate

- It is recommended that clients are disconnected from a service after a pre-determined period of inactivity. This will reduce the risk of others using the client's credential.
- When a client's session with a service has ended, there must be a process for recognising they have left or logged out in accordance with the Access Management Guidelines (see Part 4 of the Toolkit)
- The directory should be updated to show any credential activity, including client password and/or PIN changes
- A process for tracking any verification requests made (ie an audit trail) should be maintained
- CAL- 3 documents must be able to be verified with the issuing agency

4. Renewing / replacing the credential

- A CAL-3 credential would be issued with a set period of currency
- The client may be informed near to the period of expiration that the credential needs to be renewed
- If a renewal notice or other notification is sent to the client, the directory should be updated accordingly
- The notification would inform the client of relevant details, including:
  - The process required to renew the credential – eg payment of a fee, presentation of a photograph in a specified form, any authentication or POI requirement, return of the credential
  - Where to present in person, if required
  - What POI information to bring to the interview
- Once the required renewal procedures have been completed and the new credential has been renewed, the directory should be updated accordingly

5. Cancelling and/or replacing lost, stolen or damaged credential

- A credential may be replaced prior to its expiry in situations where it is damaged or otherwise rendered unusable, but only on the basis of an established authentication process to verify the identity of the person requesting the replacement
- The client would be required to report the loss or theft of a credential as soon as practicable after becoming aware of the event
- Replacing a lost or stolen credential poses a higher risk than replacing a damaged or unusable credential
- A credential may be replaced within the set renewal period in situations where it has been either lost or stolen, but only on the basis of an established authentication process that verifies the identity of the person requesting the replacement.
- On receiving notification of the loss or theft of a credential, the agency should:
  - Cancel the credential immediately or place a notice on the credential warning that the status of the credential is under investigation; and
  - Update the directory to indicate the cancellation of credential, together with any other relevant details
- The client should be informed on what steps need to be taken to obtain a replacement credential (see sub-section 4 above)

- Where a client reports that the credential is extensively damaged rendering it unusable (eg broken in half), the agency should:
  - Require the client to present the damaged credential in person at a designated place
  - Retain the damaged credential
  - Provide the client with details of what requirements will apply – eg completion of statutory declaration, presentation of identification information, provision of photograph, etc
- Sub-section 4 above provides guidelines for the reissuing of damaged credentials
- When replacing a lost, stolen or damaged credential, it is desirable that a unique identification number or other feature be incorporated in the replacement credential to indicate its status as a replacement
- Where a credential has been returned and a replacement issued, the directory should be updated accordingly

6. Exceptions

As noted in Part 2 of the Toolkit, agencies will from time to time enrol clients who are not able to meet the required Identity Registration Assurance Level. In instances where a non-standard enrolment process is completed, it may also be necessary to issue a credential.

6.1 Non-standard applications

For medium to high risk situations, a credential issued under a non-standard identity assessment process should be issued only as a last resort and the risk associated with the transaction carefully considered by the agency or specific business unit responsible for the service or transaction.

One option is to issue the applicant with a restricted identity credential, which entitles the holder to access the issuing agency's services only, or which is issued only as a temporary credential with a limited period of currency.

6.2 Service-only credential

Where an agency has the need to implement the use of a service-only or temporary credential, it may be appropriate for the registering agency to apply limitations on the service-only or temporary credential, such as:

- It would lapse after a limited period of time, either when the individual was able to register to IRAL-3, or when the registration expires
- It would be issued for the sole purpose of doing business with the registering agency

In all instances of non-standard applications, the key consideration for the registering agency is that the applicant be required to provide evidence or documentation to the satisfaction of the registering agency and to a level determined by that agency but within the required constraints for an IRAL-3 registration.

Credential Assurance Level 2 Guidelines

Suitable for:

The following processes are relevant for any of the credentials or documents issued under the Identity Registration Assurance Level 2 in Part 2 of the Identity and Access Management Toolkit.

1. Generating the credential and updating the directory

- An issuing order to generate a credential will be made only on receipt of a written request from the identity enrolment agency
- The order should contain relevant information as required by the agency, and consistent with Credential Assurance Level 2 (CAL-2) standards or requirements, including:
  - Unique identifying number for the client or service
  - The client's name in the format to be included on the credential (and consistent with agreed whole-of-government requirements – eg AS4590)
  - Other relevant client data, such as date of birth, address, etc, required by the agency
- If not already created, a client record should be created in an agency client information store, based on the information provided in the issuing order (see *Information Security Guidelines*, Version 4.0, February 2008)
- If the credential is to be produced by an external supplier, the order needs to be submitted in a secure manner, as provided under the *Information Security Guidelines* (Version 4.0, February 2008, section 6.3.1) and in accordance with the requirements of the *Personal Information Protection Act 2004* (available at www.thelaw.tas.gov.au).
- Once produced, the credential should be checked prior to distribution to the client to verify the accuracy of information printed on the credential against the initial issuing order, as well as for the fitness for purpose of the security features
- When the credential is ready to send to the client, the client's record in the agency directory needs to be updated to establish the link between the client and the credential
- Prior to delivery of the credential to the client, it is recommended it be stored securely in accordance with the *Information Security Guidelines* (Section 3, Record Security Guidelines, and Section 4, Physical Security Guidelines)

2. Delivery of the credential

- The credential would be delivered to the client by:
  - Post – normal mail will suffice
  - Collected in person by the client – a record of collection should be noted
  - Online – via email, providing details of the relevant username and password and/or PIN for the credential (for electronic credentials)
  - SMS – advising username and password and/or PIN for the credential (for electronic credentials)
- A credential may be instantly issued while the client waits

- If this approach is taken, it should be based on appropriate authentication and enrolment procedures to ensure that the identity being asserted at enrolment is correctly attributed
- The agency directory would be updated to show that the credential has been issued to the client
- At the time of issuing the credential, clients should be provided with details on what actions they are required to take to report lost, stolen or damaged credentials

3. Recognising and verifying the credential

- Acceptable methods for identifying and/or verifying a CAL-2 credential include:
  - Online transaction – accompanied by a password, PIN, cryptographic keys and/or digital certificate
    Online transactions will require validation of the electronic credential using appropriate authentication protocols
  - Telephone transaction – by supplying the name on card, service and/or credential number, and keypad entry of PIN (if required)
    Telephone transactions will require a knowledge-based authentication process. Knowledge-based authentication is not as secure as credential-based authentication and should be carefully considered in relation to the Level 4 assurance process. Information to enable knowledge-.based authentication needs to be collected during the enrolment process.
  - In person transaction – accompanied by sighting the credential and the use of password or PIN (if required)
    In person transactions may use either credential-based or knowledge-based authentication. Credential-based authentication is recommended for Level 4 assurance processes.
- Where a client's transaction with the system is over an extended period of time, for example longer than 30 minutes, or where the client moves to another secure area within the system, they should be required to re-authenticate
- It is recommended that clients are disconnected from a service after a pre-determined period of inactivity. This will reduce the risk of others using the client's credential
- When a client's session with a service has ended, there must be a process for recognising they have left or logged out in accordance with the Access Management Guidelines (see Part 4 of the Toolkit)
- The directory should be updated to show any credential activity, including client password and/or PIN changes
- A process for tracking any verification requests made (ie an audit trail) should be maintained
- CAL- 2 documents must be able to be verified with the issuing agency

4. Renewing / replacing the credential

- A CAL-2 credential may be issued with a set period of currency
- The client may be informed near to the period of expiration that the credential needs to be renewed
- If a renewal notice or other form of notification is sent to the client, the directory should be updated accordingly
- The notification would inform the client of relevant details, including:
  - The process required to renew the credential – eg payment of a fee, any authentication or POI requirement, return of the credential

  - Where to present in person, if required
  - What POI information to bring to the interview, if required
- Once the required renewal procedures have been completed and the new credential has been renewed, the directory should be updated accordingly

5. Cancelling and/or replacement of a lost, stolen or damaged credential

- A credential may be replaced before the expiry period in situations where it is damaged or rendered unusable
- It is desirable that in these situations, the replacement credential is issued in accordance with an established process to verify the identity of the person requesting the replacement
- Replacing a lost or stolen credential poses a higher risk than replacing a damaged or unusable credential
- A credential may be replaced within the set renewal period in situations where it has been either lost or stolen. It is desirable that in these situations, the replacement credential is issued in accordance with an established process to verify the identity of the person requesting the replacement
- A client should be required to report the loss or theft of a credential as soon as practicable after the event
- On receiving notification of the loss or theft of a credential, the agency should:
  - Cancel the credential immediately
  - Alternatively, place a notice in the directory warning that the status of the credential is currently inactive
  - Update the directory to indicate the cancellation of credential, together with any other relevant details
- The client should be informed on what steps they need to take to obtain a replacement credential (see sub-section 4 above)
- Where a client reports that the credential is extensively damaged (eg broken in half), the agency may:
  - Require that the damaged credential be presented in person at a designated place
  - Retain the damaged credential
  - Provide the client with details of what procedures will apply in order to receive a replacement credential – eg completion of statutory declaration, presentation of identification information, etc
- Sub-section 4 above provides guidelines for the reissuing of damaged credentials
- When replacing a lost, stolen or damaged credential, a unique identification number or other feature could be incorporated in the replacement credential to indicate its status as a replacement
- Where a credential has been returned and a replacement issued, the directory should be updated accordingly

6. Exceptions

Where an agency has the need to implement the use of a service-only or temporary credential, it may be appropriate for the registering agency to apply limitations on the service-only or temporary credential, such as:

- It would lapse after a limited period of time, either when the individual was able to register to IRAL-2, or when the registration expires
- It would be issued for the sole purpose of doing business with the registering agency

In all instances of non-standard applications, the key consideration for the registering agency is that the applicant be required to provide evidence or documentation to the satisfaction of the registering agency and to a level determined by that agency but within the required constraints for an IRAL-2 registration.

Credential Assurance Level 1 Guidelines

Suitable for:

The following processes are relevant for any of the credentials or documents issued under the Identity Registration Assurance Level 1 in Part 2 of the Identity and Access Management Toolkit.

1. Generating the credential and updating the directory

- Where a credential is to be issued, it may be appropriate to require a written request from the identity enrolment agency prior to generating a credential
- The issuing order should contain relevant information as required by the agency, and which is consistent with Credential Assurance Level 1 (CAL-1) standards or requirements, such as:
  - The client's name in the format to be included on the credential (if required)
  - Any other relevant client data required by the agency
- Other features, such as a unique identifying number for the service and/or the credential may be included if required
- Where a credential is to be issued under the client's name, and if not already created, a client record may be created in an agency directory, based on the information provided in the issuing order (see *Information Security Guidelines,* Version 4.0, February 2008)
- When the credential is ready to send to the client, the client's record in the agency directory needs to be updated to establish the link between the client and the credential

2. Delivery and activation of the credential

- The credential may be delivered to the client by either:
  - Post – normal mail will suffice
  - Collected in person by the client – some identification may be required
  - Online – via email, providing details of the relevant username and password and/or PIN for the credential (for electronic credentials)
  - SMS – advising username and password and/or PIN for the credential (for electronic credentials)
- A credential may be instantly issued while the client waits
- In this circumstance, no identification would be required where the credential is not being issued in the client's name
- Where appropriate, the agency directory would be updated to show that the credential has been issued to the client
- At the time of issuing the credential, the client would be provided with details on what actions they need to take to report the loss, theft or damage to the credential

3. Recognising and verifying the credential

- Acceptable methods for identifying and/or verifying a CAL-1 credential would include:
  - Online transaction – unique identifier for the service or credential
  - In person transaction – sighting the credential
  - Telephone transaction – unique identifier for the service or credential

4. Renewing / replacing the credential

- A CAL-1 credential may be issued with a set period of currency
- The client could be informed near to the period of expiration that the credential needs to be renewed, if required by the agency
- If a renewal notice or other form of notification is to be sent to the client, the directory may be updated accordingly
- The notification could inform the client of relevant details, including:
  - The process required to renew the credential – eg payment of a fee, return of the credential
  - Where to present in person, if required
- Once the required renewal procedures have been completed and the new credential has been renewed, the directory may be updated accordingly
- A credential may be replaced without using a renewal process

5. Cancelling and/or replacing lost, stolen or damaged credential

- On receiving notification of the loss or theft of a credential, the agency may decide to cancel the credential
- If a credential is cancelled, the directory may be updated accordingly
- The client would be informed of the steps needed to be taken to obtain a replacement credential (see sub-section 4 above)
- Where a client reports that the credential is extensively damaged (eg broken in half), the agency may:
  - Request the client to return the damaged credential to a designated place
  - Retain the damaged credential
- Sub-section 4 above provides guidelines for the reissuing of damaged credentials
- Where a credential has been returned and a replacement issued, the directory may be updated accordingly

6. Exceptions

As the process for CAL-1 credentials applies to low risk or pseudonymous transactions, no exception procedures are required.

Credential Assurance Level 0 Guidelines

Suitable for:

The following processes are generally relevant for any anonymous transactions where no identity assessment is required due to the minimal risk involved with the transaction, and a credential is not issued.

1. Generating the credential and updating the directory

- Due to the anonymous nature of Credential Assurance Level 0 (CAL-0) transactions, an identity enrolment process may not be applicable (though in some cases, an application form may be completed)
- A credential would be issued based on the relevant procedures for the CAL-0 transaction, such as payment of a fee, completion of an application form, etc
- There are no directory data requirements

2. Delivery and activation of the credential

- CAL-0 transactions are anonymous and therefore an identity credential is not required
- However, some form of credential may be issued to facilitate access to a service or other entitlement – ie there is no identity linked to the credential

3. Recognising and verifying the credential

- Where a credential is issued in relation to a CAL-0 transaction, it would not incorporate an identity component
- A service-only credential would be verified by a unique identifier for the credential, such as a service or credential number

4. Renewing / replacing the credential

- As a CAL-0 credential relates to anonymous transactions, it is issued on an as required basis and is not renewable (ie it would simply be replaced)
- A CAL-0 credential would normally be useable for a single use, or other multiple uses as determined by the credential issuing agency

5. Cancelling and/or replacement of lost, stolen or damaged credential

- Where a credential has been issued for multiple use purposes, loss or damage would be reported and, where appropriate, a replacement card issued (see sub-section 4)

6. Exceptions

As the process for CAL- 0 applies to anonymous transactions, no exception procedures are required.

Summary of Credential Assurance Levels

Process Required	Notes	Credential Assurance Levels				
		CAL-0	CAL-1	CAL-2	CAL-3	CAL-4
		Negligible Risk	Minimal Risk	Low Risk	Moderate Risk	High Risk
Type of credential	Level of security features to be incorporated in the credential	None	Weak level security features	Medium level security features	High level security features	Very high level security features
Identifying and verifying the credential	Method of identifying the credential and being able to verify its authenticity	None	Weak level verification	Medium level verification with identifier(s)	High level verification with multiple identifiers	Very high level verification with multiple strong identifiers
Renewal / replacement of credential	Security requirements in relation to regular renewal, as well as in relation to loss or damage	None	No set expiry Weak renewal procedure	No set expiry Medium renewal procedure	Set expiry High renewal procedure	Set expiry Very high renewal procedure

Section 2

Identity Credential Standards

Standard 1
Non-Electronic Credentials Standard

- Non-electronic credentials are credentials that can be touched physically – such as a driver's licence, a senior's card
- The standard details the required minimum level of security features to be incorporated in the credential for each Credential Assurance Level (ie CAL-4,CAL-3 and CAL-2)
- An agency will select the appropriate security features to be incorporated in the credential they intend issuing based on the assessed risk or assurance level determined in relation to Part 1 of the Toolkit
- An agency may decide to incorporate more security features in the final credential than suggested by the standard (however, this would potentially increase the cost of the credential, and may provide a greater than necessary level of security)
- Knowing what security features a credential will contain can help with the design and style of a credential

CAL-4, CAL-3 and CAL-2 credentials

- The standard details the types of features that are applicable to non-electronic credentials assessed at these levels
- The types of features that can be incorporated in a non-electronic credential for each level are grouped in terms of covert, semi-covert and overt features:
  - **Covert –** represents the third line of document inspection – ie a specialist may be required to conduct a detailed in-depth examination of a document using special equipment and knowledge
  - **Semi-covert –** represents the second line of document examination – ie a trained employee using simple equipment such as a magnifying glass, ultra-violet light, infra-red lamp, etc
  - **Overt –** represents the first line of document examination undertaken by a trained employee using sight and/or touch
- Where all three of these terms are indicated, a credential will use at least one of each
- The standard is to be used in conjunction with Step 4 in Part 1 of the Toolkit
- When an agency is deciding upon which credential is required, a number of questions are applicable – eg what security features are required on the credential

CAL-1 and CAL-0 credentials

- The standard does not provide requirements for CAL-1 or CAL-0 non-electronic credentials as the associated risk involved does not warrant a standard
- An agency may decide to incorporate any security feature they deem to be appropriate in credentials assessed at these levels
- Electronic credentials do have minimum requirements and a standard is provided
- The standard does not provide guidance selecting and appointing a credential printing or development company – this is a process that would be dealt with as part of the agency's normal procurement guidelines

How to use the standard

- To use the standard, an agency must first know:
  (a) The assurance or risk level for their credential – as determined by applying Part 1 of the Toolkit
  (b) The type of credential intended to be issued (eg paper certificate, plastic card)
- The standard shows minimum requirements for each of the Credential Assurance Levels. For example a CAL-4 non-electronic credential must have as a minimum, the following:

  From the covert group:
  - At least two security inks where one of these must be a taggant ink
  - It must use fluorescent or security thread in paper documents
  - It must contain two other features from the covert group

  From the semi-covert group:
  - It requires at least three different high-resolution printing processes
  - It must contain at least these three printing techniques: Guilloche pattern, Latent image, and Micro printing

  From the overt group:
  - It must contain all seven overt features

  It may also incorporate an electronic chip which incorporates a JPEG facial image

The following standards have been based on the National Identity Security Strategy paper, *Security Standards for Proof of Identity Documents*, which is provided as Appendix 2 to the Toolkit. This document should be referred to for interpretation of the technical terms used in the Credential Management Standard.

Non-Electronic Credentials Standard
Credential Assurance Level 4 documents

	Feature	Recommended minimum features
Covert	• Hidden image • *Paper documents*: Fluorescent fibre paper • *Paper documents*: Security fibres • *Paper documents* Security threads • *Plastic cards*: Fluorescent printed areas embedded on card surface • Screen angle modulation • Security ink	Include two security inks including at least one *taggant* ink Include fluorescent or security fibre or security threads in paper documents Include two other 'covert' features
Semi-covert	• High resolution printing processes	Include at least three printing processes as detailed in Appendix 2
	• Guilloche pattern • Latent image • Microprinting	Include all three of these printing features. Other additional printing features are also available for inclusion (See Appendix 2)
Overt	• Bearer's signature • Digital facial image • Embossing • Diffractive OVD (DOVD) • *Paper documents*: Watermark • *Plastic cards*: Watermark equivalent • Shadow / secondary image • Unique identifier	Include all seven of these 'overt' features – See Appendix 2 on the effects to be included in the DOVD device
Electronic chip	• Contact or contactless electronic chip containing JPEG facial image, including Public Key Infrastructure (PKI) and Basic Access Control (BAC)	An electronic chip which incorporates a JPEG facial image may be included

Non-Electronic Credentials Standard
Credential Assurance Level 3 documents

	Feature	Recommended minimum features
Covert	• Security ink • Screen angle modulation • *Paper documents*: Fluorescent fibre paper • *Plastic cards*: Fluorescent printed areas embedded on the card surface • Hidden image	At least one security ink may be included At least one other 'covert' feature may be included
Semi-covert	• High resolution printing processes	Include at least two printing processes as detailed in Appendix 2
	• Micro printing • Guilloche pattern • Latent image	Include two of these printing features. Other additional printing features are also available for inclusion. (See Appendix 2)
Overt	• Bearer's signature • Digital facial image • Embossing • Diffractive OVD (DOVD) • *Paper documents*: Watermark • *Plastic cards*: Watermark equivalent • Shadow / secondary image • Unique identifier	Include a DOVD – see Appendix 2 on the effects to be included in the DOVD Include a unique identifier Include digital facial image The bearer's signature may be included At least one other 'overt' feature may be included

Non-Electronic Credentials Standard
Credential Assurance Level 2 documents

	Feature	Recommended minimum features
Semi-covert	• High resolution printing processes	At least one printing process may be included as detailed in Appendix 2
	• Guilloche pattern • Latent image • Micro printing	At least one of these printing features may be included Other additional security printing features are also available for inclusion (See Appendix 2)
Overt	• Embossing • Optically variable ink • *Paper documents*: Watermark • *Plastic cards*: Watermark equivalent • Shadow image • Unique identifier	Include a unique identifier At least one or more other 'overt' feature may be included

Standard 2
Electronic Credentials Standard

- Electronic credentials are credentials that cannot be physically touched – eg a username with associated password
- This section details what security feature standards agencies are required to have for these types of credentials

How to use this standard

- To use the standard, an agency must first know:
  (a) The assurance or risk level for their credential – as determined by applying Part 1 of the Toolkit
  (b) The type of credential intended to be issued (eg One-time passwords generated within a token)
- The standard shows minimum requirements for each of the Credential Assurance Levels. For example, a CAL-4 electronic credential must have as a minimum, the following:
  - High quality biometric

  Use this required biometric with a:

  - Digital signature, that has the private key stored in hardware and is PIN protected

Electronic Credentials Standard
CAL-4 – High assurance, high confidence in the assertion

e-Authentication Mechanism	Use	Variables determining strength of mechanism
Required		
A high quality biometric	Identity authentication[2]	Nature of biometric
Use the required biometric with either of the following e-Authentication mechanisms:		
Digital signature, with the private key stored in hardware and PIN-protected	Identity and transaction authentication	Method of PIN entry, security of chip
Using digital signatures, with the private key stored in hardware and biometrics-protected	Identity and transaction authentication	Method of biometric use, security of chip

[2] Identity and transaction authentication refers to the verification of a person who is trying to use a service by checking the identity and credential allowing them to use the service

Electronic Credentials Standard
CAL-3 – Moderate assurance, moderate confidence in the assertion

e-Authentication Mechanism	Use	Variables determining strength of mechanism
Required		
A low quality biometric	Identity authentication	
Can use higher quality biometric if desired		
A high quality biometric	Identity authentication	Nature of biometric
Use the required biometric with any of the e-Authentication mechanisms below:		
Call back to the pre-registered address for that username • Voice • SMS OTP • email OTP	Identity authentication	Security of channel
Digital signature, with the private key stored in approved software	Identity and transaction authentication	Password policy
One-time passwords generated within a token	Identity authentication	Security of device, PIN protection policy
Challenge – Response Token	Identity and transaction authentication	Security of device, PIN protection policy

Electronic Credentials Standard
CAL-2 – Low assurance, some confidence in the assertion

e-Authentication Mechanism	Use	Variables determining strength of mechanism
Traditional Secret Password	Basic authentication	Password policy
Check of the origin against a pre-registered origin for that username • Caller-ID • Internet Protocol address	Basic authentication	

Electronic Credentials Standard
CAL-1 – Minimal assurance, little requirement for confidence in the assertion

e-Authentication Mechanism	Use	Variables determining strength of mechanism
Password stored in persistent cookies	Very basic identification	

Electronic Credentials Standard
CAL-0 – No assurance, no confidence in the assertion

No standard is applicable as there is no requirement for a credential to be issued.